UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF ILLINOIS

IN THE MATTER OF THE SEARCH OF A WHITE APPLE IPHONE IN A CLEAR AND BLACK PHONE CASE SEIZED FROM ELIJIAH SMITH CURRENTLY IN THE CUSTODY OF THE FBI	)	No. 23-mj-7125-MAB
	)	**FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Omba Ngoma, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of an electronic device – described in Attachment A, which is currently in law enforcement possession, and the extraction from that device of electronically stored information described in Attachment B.

2. I am a Special Agent (SA) with the United States Department of Justice, Federal Bureau of Investigation ("FBI"), currently assigned to the Springfield Division, Fairview Heights Resident Agency. I have been so employed since January 2018. As a Special Agent, I have graduated from the FBI Academy. As such, I am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure. In my capacity as a Special Agent, I am responsible for investigating violations of federal statutes over which the FBI has investigative jurisdiction, to include violations relating to firearms, controlled substances, violent crime, organized crime, public corruption, national security investigations, kidnapping, and bank robberies. During my tenure with the FBI, I have participated in investigations involving national security, bank robbery, crimes involving firearms and controlled substances. I am

familiar with and have used normal methods of investigation, including, but not limited to, visual and electronic surveillance, interviewing witnesses and defendants, reviewing social media accounts, utilization of cellular telephone data, and the utilization of confidential informants and undercover agents. Prior to being a Special Agent with FBI, I was employed as a police officer, tactical response team operator, and personal security to the Director of the National Geospatial-Intelligence Agency (NGA) in Missouri from January 2016 to January 2018. Prior to that, I was employed as a Police Officer with the St. Louis Metropolitan Police Department in Missouri from October 2014 to January 2016. I started my civilian law enforcement career as a Police Officer with the City of Venice in Illinois from January 2012 to October 2014. I also serve as a reserve Special Agent with the United States Army Criminal Investigation Division (USACID.) I have served in that capacity since February 2016.

3. The facts and information contained in this affidavit are based on my personal knowledge, information obtained from other law enforcement officers/agents, witnesses and/or victims. All observations referenced in this affidavit that were not personally made by me were relayed to me by the person(s) who made such observations or in reports that detailed the events described by that person(s). This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of **18 U.S.C. § 2119 Carjacking** and **18 USC § 924(c) Use of a Firearm During a Crime of Violence** have been committed. Additionally, there is probable cause to search the information described in Attachment A for evidence of crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICES

The property to be searched (hereinafter the **"SUBJECT DEVICE",** described below, and described and depicted in ATTACHMENT A, is currently located at the FBI Fairview Heights Resident Agency, located at 16 Executive Drive, Fairview Heights, IL 62208, is as follows:

White Apple iPhone with clear and black case

5. Following its seizure, as described below, the **SUBJECT DEVICE** was securely stored with Illinois State Police (ISP) then transferred and securely stored at the FBI Fairview Heights Resident Agency. Prior to seizing the **SUBJECT DEVICE**, Smith powered off the device. The **SUBJECT DEVICE** has not been forensically/physically examined or altered in any way since their seizure.

6. The applied-for warrant would authorize the forensic/physical examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Subscriber Identity Module ("SIM") card: A SIM card is a smart card inside a mobile phone, carrying an identification number unique to the owner, storing personal data, and preventing operation if removed. A SIM card is an integrated

circuit that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

d. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations.

PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on my training, experience, and research, I know that the **SUBJECT DEVICE** has the capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, and/or can access the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the **SUBJECT DEVICE**.

PROBABLE CAUSE

1. On Sunday, August 27, 2022, at approximately 6:43 a.m., the body of Harriett K. Childers (B/F, 10/23/72) was located in the street in front of 1855 Gaty Avenue in East St. Louis,

Illinois, within the Southern District of Illinois. Childers died of 2 gunshot wounds to the back side of her head. Her car was located that morning near Eco Recycling Solutions located at 225 S. Main Street in East St. Louis. Childers was driving for Uber at the time of her murder. At 12:32 a.m., Childers agreed to pick up a fare from the apartment building at 3009 E. B Street in Belleville, Illinois. Childers picked up the fare at 12:41 a.m. The following customer information was provided by Uber related to that fare:

Name: Keon Bunker
Phone Number: 618-531-7211 **("the Suspect Phone")**
Email: yoazzigot3@gmail.com
Billing Info: Visa, Sutton Bank, CC#: 4403-93XX-XXXX-8406, Exp. Date: 7/27
The initial requested drop off location was 1611 Gaty Avenue in East St. Louis. According to Uber, the drop off was completed at 1:05 a.m. at N. 18th Street and Cleveland Avenue in East St. Louis.

2. Investigators could not identify the name "Keon Bunker" in any law enforcement or open-source database. ISP Analysts determined the phone number for the Uber Account, 618-531-7211, was linked to the SnapChat account identified as "nlmbkye," with a display name of "Nuskigang Kyeion."

3. Diane Hill, a witness identified as having a connection to **SUSPECT PHONE** was interviewed. Hill showed law enforcement a conversation through Facebook messenger with "NuskiMobb Kyeion". In that conversation, "NuskiMobb Kyeion" who Hill knew to be Kyeion Stidimire, requested Hill pay his phone bill and identified his phone number as **SUSPECT PHONE** on June 25, 2022. Through a review of Facebook, ISP analysts identified a Facebook profile for NuskiMobb Kyeion (ID: 100013665879391). The photos in that account are

consistent with Kyeion L. Stidimire (B/M, DOB: 10/01/02) and connected to the T-Mobile phone number used to create the Uber Account and request the ride from victim Childers.

4. Kyeion Stidimire was questioned by law enforcement. Stidmire acknowledged his phone number and Facebook account. Stidimire identified "Jmon" last name unknown as the individual who provided him with the **SUSPECT PHONE**. Stidimire stated he no longer possessed the **SUSPECT PHONE** and had stopped using it approximately one month prior. Stidimire estimated he used the phone for 3 months.

5. A bank account used by the suspect in the carjacking was identified from Uber records as returning to Sutton Bank. An Illinois state subpoena was served on Sutton Bank for subscriber and transaction information for that account. Records provided in response to the subpoena indicated that the Sutton Bank account documented a person and address for a bank card for the suspect account sent out on June 3, 2022. That information included:

i. Recipient name: Jmon Falconer

ii. Recipient Address: 18 Yorkshire Lane Apt. L, Belleville, Illinois 62221

6. Based on analysis of call detail records for **SUSPECT PHONE**, and additional law enforcement investigation into Jmon Falconer, law enforcement identified Elijiah Smith, Valencia Ransom, and Destiny Johnson as individuals with potential information relating to Jmon Falconer and the events of August 26 and 27, 2022.

7. Cellular phone records show Johnson, Smith, and the suspect's phones arriving in the same area of East Saint Louis at approximately 1:45 A.M. This is consistent with the location of where the victim's vehicle was discarded and the time period after the carjacking.

8. During an interview of Valencia Ransom identified her home address as 18 Yorkshire Lane, Belleville, Illinois. Ransom identified Elijiah Smith as her boyfriend and Jmon Falconer as a Smith's relative who also spent time at her residence. Ransom identified a still photograph of Smith and Falconer together. That still photograph came from a video taken on August 26, 2022, prior to the carjacking and homicide. That photograph showed Falconer with a firearm. Ransom denied knowledge of a carjacking, denied observing Falconer with a firearm, and denied knowledge of any crimes Falconer had committed.

9. During an interview of Destiny Johnson, law enforcement learned Johnson accompanied Falconer to East Saint Louis on August 27, 2022, and was told by Falconer that he had earlier been involved in an Uber carjacking that resulted in killing the Uber driver. Johnson identified two individuals that met Falconer and Johnson in East Saint Louis to pick them up after Falconer discarded the victim's car. Johnson further described Elijiah Smith as an individual who was contacted by the suspect using Johnson's phone and directed to the specified location in East Saint Louis. Johnson identified Valencia Ransom and Elijiah Smith as the individuals who picked up her and Falconer from East Saint Louis. Johnson additionally described the suspect providing his firearm to Smith. Smith drove Johnson and Falconer to her residence and dropped them off. Smith and Ransom left with the firearm.

10. During an interview with Elijiah Smith, Smith identified his Instagram name. Social media records show that Smith's Instagram account contacted Falconer during the early morning hours after the homicide. Smith identified Falconer as his cousin and Ransom as one of his girlfriends. Smith requested a lawyer when questioned about the events of August 26-27, 2022. Smith's white Apple iPhone (SUBJECT DEVICE) was seized as evidence.

11. Phone records corroborated that Smith communicated with Johnson's phone during the early morning hours of August 27, 2022, after the carjacking/homicide.

What and Why Targets use Electronic Devices like the Subject Electronic Device

9. During your affiant's career as a law enforcement officer, your Affiant has conducted and/or participated in violent crime investigations. Based on your Affiant's training and experience in such investigations, and evidence received from this investigation, your Affiant and other members of the investigative team, know that individuals committing violent crime often communicate with each other utilizing cellular telephones and other electronic devices to facilitate the overall scheme of their illicit endeavors. Individual engaged in violent crime often communicate before, during, and after to facilitate their crimes, receive assistance in covering their crimes, or communicate with others to limit other witnesses sharing information about their crimes.

10. Individuals engaged in the activities described in this affidavit use electronic devices and mobile phones for a variety of reasons including but not limited to:

(a) Accessing contact lists of associates, confederates, and third parties;

(b) Targets take pictures and videos of themselves and associates, to memorialize their activities and fruits of their illicit activities such as contraband and firearms.. They use the images or to brag to other confederates. These individuals frequently maintain these photographs on their electronic devices and, as described below, often post the images on social media.

(c) Criminals use the devices for online social media platforms such as Facebook, Twitter, Snapchat, etc. They communicate with their associates and confederates over such

platforms. They post and display images and videos of contraband, fruits of their crimes, wealth, and otherwise memorialize criminal activities.

(d) Criminals also may use devices to navigate to specific locations involved or connected to the crime.

11. In summary, electronic devices such as the **SUBJECT DEVICE** described herein and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society. Thus, there is reason to believe that the **SUBJECT DEVICE** could have been used in conjunction with the events described herein. The **SUBJECT DEVICE** themselves operate as instrumentalities of the crimes described herein.

What Can Be Recovered From the Electronic Devices

12. Based on training and experience, your Affiant knows that forensic examinations may be performed on electronic devices such as mobile phones tablets and, computers. Devices use internal fixed memory, SIM cards, or removable memory that stores the previously described information. It takes specialized training and experience along with software and hardware to perform forensic examinations and analysis of such devices and memory to retrieve this information. A forensic examiner may be able to recover evidence of the illegal activities described in this affidavit, including: user attribution, photographs, text messages, videos, phone and address books, call history, and geographical location data.

13. Further, electronic devices such as those identified in this affidavit can store information for long periods of time. These devices contain files or remnants of files that can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or

years later using forensic tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. Additionally, this information can carry over from one device to another if the user replaces the device used at the time of the crime.

14. Information that is electronically stored on the **SUBJECT DEVICE** serves as direct evidence of the crimes described in this warrant. Forensic analysis may demonstrate how the **SUBJECT DEVICE** was used, the purpose of its use, who used it, and when. There is probable cause to believe that such evidence will be on the **SUBJECT DEVICE.** Data on the **SUBJECT DEVICE** will likely also show who used or controlled the **SUBJECT DEVICE**. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing an arrest warrant and subsequent search warrant at a residence. Lastly, data on the **SUBJECT DEVICE** can show how the **SUBJECT DEVICE** was used as an instrumentality of the crimes.

15. The **SUBJECT DEVICE** is currently in the possession of the FBI**.** They came into FBI's possession in the following way: **SUBJECT DEVICE** was transferred on July 27, 2023 from ISP. ISP had retained custody of the **SUBJECT DEVICE** from its seizure on July 24, 2023. The **SUBJECT DEVICE** has remained in the possession of the FBI, since the seizure as described above.

16. In my training and experience, I know that the **SUBJECT DEVICE** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of ISP and FBI. Therefore, there is probable cause to believe the files and evidence on the devices have been unchanged since July 24, 2023, when they were seized. There is therefore still probable cause to believe that the Device contains electronic files evidencing criminal activity.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

20. Your Affiant submits that this affidavit supports probable cause for a search warrant authorizing the examination of the Subject Device described in Attachment A to seek the items described in Attachment B.

21. Because this warrant seeks only permission to examine Subject Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

22. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These

documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

Elmba Ngom
Special Agent
Federal Bureau of Investigations

Sworn to, attested to, or affirmed before me via reliable electronic means on July 28, 2023

Mark A. Beatty

The Honorable Mark A. Beatty
United States Magistrate Judge
Southern District of Illinois

ATTACHMENT A

Property to be searched

The property to be searched (hereinafter collectively the **"SUBJECT DEVICE"** is described as follows. The **SUBJECT DEVICE** is currently located at FBI Fairview Heights Resident Agency, located at 16 Executive Drive, Suite 305, Fairview Heights, IL 62208. This warrant authorizes the forensic examination of the **SUBJECT DEVICE** for the purpose of identifying the electronically stored information described in Attachment B.

SUBJECT DEVICE

White Apple iPhone with clear and black case

ATTACHMENT B

Property to be seized

1. All records and information relating to violations of Title 18 United States Code 211 and 18 United States Code 924(c), that constitutes fruits, evidence, and instrumentalities of those violations, including, but not limited to:

   a. Any information relating to communications between SMITH and individuals involved in the above-mentioned crimes or with knowledge of the above-mentioned crimes.

   b. Any information recording SMITH's past travel.

   c. Any information as to the location, activities, searches, or communications that occurred on August 26, 2022 and after related to the above-mentioned crimes.

   d. Any information related to firearms and ammunition.

   e. Any information related to communications about the ongoing investigation and contact with witnesses to the above discussed investigation.

2. Evidence of user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, location information, and browsing history.